MEET THE EXPERT Q&A

How to Build an IAM Transformation Programme

Mark Gleeson - IAM Transformation Programme Manager

Give us a brief overview of the programme you're currently working on?

I'm currently running a global identity & access management transformation (IAM) programme for a large financial services business. This is my third large-scale transformation programme – each is slightly different. In this case, we are effectively transforming all elements of IAM within the organisation. That includes identity governance and administration (IGA) as well as privileged access management (PAM).

I directly manage the traditional IAM side of the transformation and have a programme manager, reporting to me, that runs the PAM delivery. We have divided the transformation in this way to ensure both areas get equal focus, whilst keeping the overall delivery aligned.

On the IAM side we look after joiners, movers, leavers, recerts, access requests etc, the controls and processes that effectively manage people's day-to-day access within the organisation, and we have PAM, which focuses purely on privileged accounts and privileged access. In the context of PAM, we concentrate on infrastructure admins, database admins, application developers etc those users with the highest level of access to databases, systems, and critical infrastructure. PAM is a huge part of IAM that requires dedicated focus. We've been mindful of this when structuring our transformation initiative.

About Mark Gleeson

Mark is a seasoned cyber security identity and access management (IAM) professional with extensive strategic and operational experience gained over 20 years at top tier global organisations.

He has worked in leadership roles within the identity space for the past 15 years with posts including the Global Head of IAM for an industry leading bank, and Global Lead for the Privileged Access Management programme within one of the world's largest insurance companies.

What are the primary drivers for businesses to invest in identity access management?

The drivers can vary from business to business. Generally, it's about reducing risk - a common theme behind any IAM investment. The programme might typically arise because of audit points. That generally occurs when you don't have a robust IAM/PAM strategy. I always say if you have a good IAM/PAM strategy the audit points take care of themselves, but you'll be surprised how many organisations don't have a 2-to-3-year vision around what they are trying to achieve in the IAM space. This can invariably lead to plugging holes with tactical fixes which ultimately cost the organisation more. However, often after a certain period of time taking this approach, an appetite is developed to implement a more coherent strategy to re-engineer to a more medium to long-term approach that creates those efficiency gains.

I also see a real focus on improving the user experience. You can have the best system in the world, but if your data isn't high quality, for example clear and meaningful role names, role descriptions etc, people won't be able to make good decisions around granting user's access. If you receive a re-certification, for example, and the data presented to you doesn't mean much, then you can't make the right decisions around whether your team members should retain that access or not, and this can be extremely frustrating for the user. Data is a big part of it. When deploying new tooling, make sure the data within is of equally high quality – because the two go hand in hand. It's about reducing risk through having the right tooling, with good data, to make the right decisions.

> **"I always say if you have a good IAM/PAM strategy the audit points take care of themselves.**

What are the biggest challenges and hurdles associated with IAM programmes and initiatives?

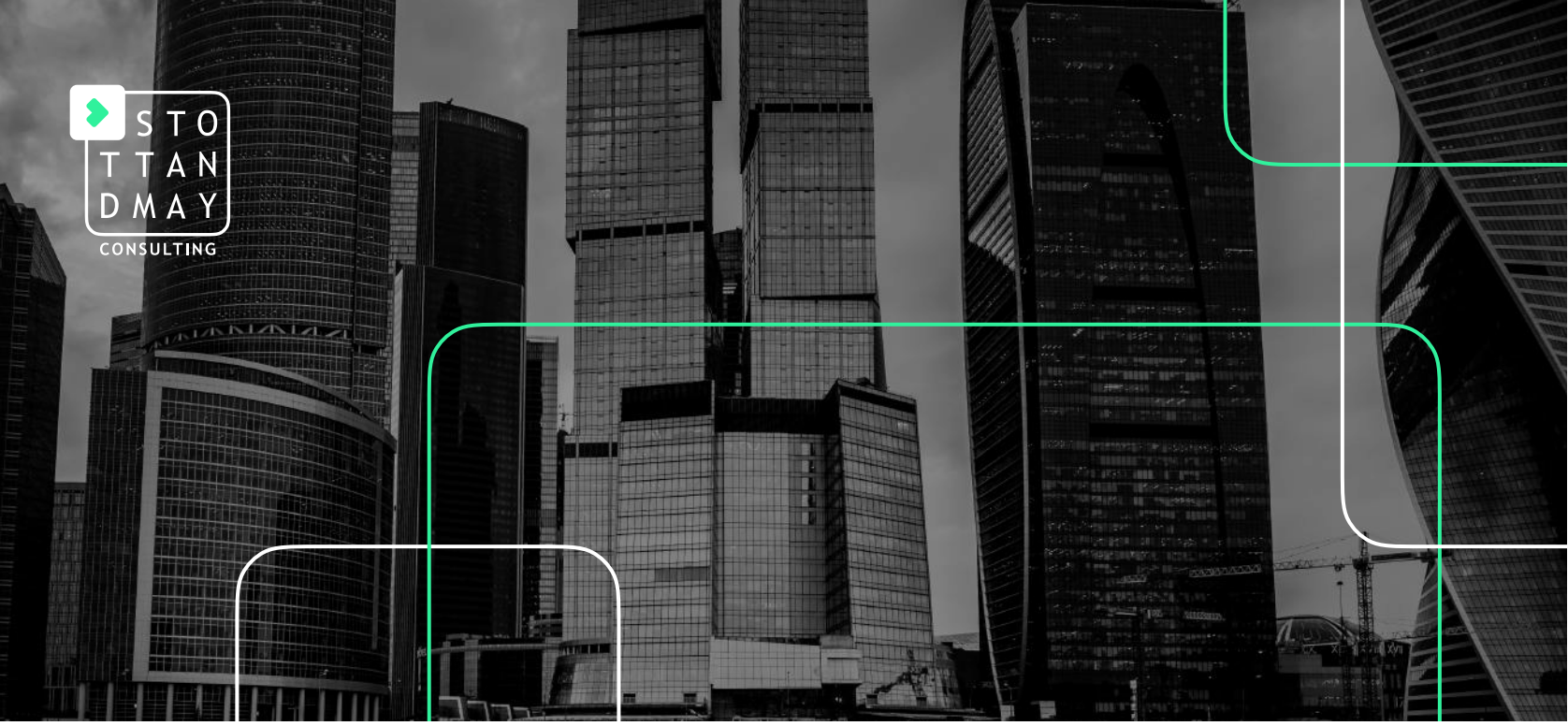
There are a few things that spring to mind. Sponsorship from senior management is crucial. A programme must be funded adequately to get the right level of resources to deliver on the core objectives. Often, I've seen big ideas, but the sponsorship and the budget are not always there, which only culminates in quick tactical fixes. I am fortunate that the client I currently work with takes IAM seriously. They want to do a full step-change around controlling user access and privileged access and have given us the tools we need to make that happen. As a result, they are getting a future-proofed long-term solution. They are thinking further than just getting through the next audit.

The culture and attitude of the organisation towards security will always be an essential consideration. Sometimes this can be cyclical, for example where a new CISO arrives that really understands the challenges, and puts a programme in place, only for them to move on and the initiative stalls. I also think there is a tendency for businesses to buy software solutions thinking they are a silver bullet to an IAM problem. Those tools are then not deployed properly or are deployed and then not used appropriately. It goes back to having the right people delivering the change, understanding the capabilities of the solution, and knowing how to integrate the functionality to reduce risk in an effective manner, particularly in large and complex environments.

What IAM solutions should transformation leaders be considering right now?

It depends on your requirements. Without knowing the scope, you could just say 'get SailPoint' or 'get CyberArk' or any of the other big solutions in this space for that matter, but that wouldn't be the right approach. For example, if you only want to secure privileged accounts within an encrypted vault, you could buy CyberArk, but that's only a small part of what the product does. So, you might be committing a lot of budget to something you may not fully utilise. Again, with SailPoint, it's a great solution, however I've seen organisations that have bought many components only to use the re-certification module. You probably could have gone for a cheaper solution if that was all you wanted. You need to know your requirements and budget and go for the product that meets your needs. There are a lot of good products out there; some do more than others, and some are more costly than others, understand the requirements first, then chose the tooling.

When I started in IAM back in the late 90's, we didn't really have any off-the-shelf IAM tools, aside from a few access request systems. In the early days we built our role management tooling internally. Over time the tools market has grown substantially, and vendors have provided platforms to help solve the problems we used to have to solve on our own. Regarding where they could go further, I think there's still some work to be done to make these tools more transparent to the user. The best security and controls are those that nobody really notices and simply churn away in the background doing their job. Over the years, the user experience will continue to improve I'm sure, with companies like CyberArk and SailPoint having already put a lot of effort into this area - ensuring IAM tooling is easier to use and less in your face.



What are the key elements that need to be in place for a team to be successful on an IAM project?

Structure and leadership are crucial to ensuring you don't end up in a position where you have lots of siloed pieces of work that are not tied together, or not moving in the same direction. It's about understanding the organisations goals to inform how the programme should be structured. Your goal might be to implement a new IGA solution. If you think about it, the software deployment and configuration is a technical piece of work, it's effectively a technology rollout. But you also need to focus on the data. All that role and entitlement level data may need cleansing across the board. There's also the business engagement, process change, business comms etc. That's a different skillset from say someone who is an expert in deploying a solution technically. Then there will be infrastructure considerations. The list goes on. People often approach IAM transformation as a technology roll out, I disagree, it's a change programme, and must be treated as such.

Based on a 2–3-year roadmap, I'd suggest breaking things down into manageable yet integrated chunks through the creation of delivery pillars. So, you might have a delivery pillar around the technology rollout where your architects and technical people converge. To satisfy the data requirements, you could create a business workstream that engages with the business and Operations teams in a less technical and more business-focused way. Then you can bring together your database and server specialists under one infrastructure pillar. This enables you to have the right people in the right place based on their skills. You can increase and decrease the projects within each delivery pillar depending on the requirements at the time, but ultimately, they all sit together within one team, creating more synergy across the projects, and more focused communication and co-ordination across the programme.

This level of structure provides clarity within the team around what they are trying to deliver, which is vital.

Outside of leadership and structure, it's all about people. Building the programme with good people who have seen what works and what doesn't and can anticipate problems and understand dependencies. Having talented IAM professionals is key, particularly those that carry some scars from the past. We've all been there and worn the t-shirt, but this is how you learn, and you ultimately bring that experience with you to the next project.

Where do you see the future of IAM going over the next few years?

I think IAM will only continue to grow and be placed at the forefront of security. There's already reasonably high awareness of the importance of IAM and PAM across financial services. Some smaller businesses are not quite there yet in terms of maturity, but across all industries, companies are waking up to the importance of protecting user identities, privileged accounts, and the need to manage access to systems more securely. I can only see IAM and certainly PAM getting bigger and bigger.

In terms of technology, I am noticing more vendors moving towards offering Cloud and SaaS based solutions. That's a bit of a shift away from the historic on-premise model. In the past some customers took the approach to create custom versions of a given tool by added their own bespoke code which over time culminated in a maintenance and support nightmare. So, most of the market leaders are now consolidating back to a more single code base offering, helping their customers by delivering SaaS based solutions through the Cloud that are less configurable, but should typically meet most of the requirements out the box.

“

You can increase and decrease the projects within each delivery pillar depending on the requirements at the time, but ultimately, they all sit together within one team, creating more synergy across the projects, and more focused communication and co-ordination across the programme. This level of structure provides clarity within the team around what they are trying to deliver, which is vital.

What advice would you give to others that are tackling the challenge of IAM transformation?

If you are coming into a new organisation you need to understand the business and get feedback on the challenges. Sometimes the problems can be broad and high-level, but some companies will have specific audit points they want to address that will ultimately shape your focus and attention. You need to understand why you were brought in and what the company is trying to achieve.

You must bring stakeholders on the journey with you. Work closely with them. Don't deliver change to them; create change with them. Remember, this is not a technology rollout, it's a change programme; a change in people, processes, and tooling. The majority of what you are trying to achieve is changing the business, and quite often ways of working that have been the same for many years. Develop strong relationships with the operations team, engrain yourself in the organisation, engage with the business, and build trust along the way as you deliver outcomes together.

How do you prepare a business for the level of change that an IAM programme can create?

It's all about being transparent. Be honest about what's required. If you need ten people to make the change, don't ask for five and fail. It's easy to say, 'we just need to bring in CyberArk and onboard accounts,' but that could be a 2–3-year project. Speak in a language the customer understands and be realistic about the outcomes you'll create, and the resources required to make that happen. You are far more likely to get buy-in when you map things out that way. Then it's about building credibility, delivering on outcomes, and maintaining project momentum.

Also, don't forget to celebrate those little wins. For example, if you deploy some new IAM capability into production, or roll out a new process or IAM control, or close out a long-standing audit point. These smaller steps in the journey add up and should be communicated on route to achieving that overall goal of reducing risk across the organisation.

What tips would you give to IAM leaders that are looking to build their internal reputation?

Trust is a big thing. If your stakeholders don't trust you, you might as well forget about it. It's not about being a salesman. It's about creating a credible roadmap, building a team, staying consistent with the narrative, and delivering on expectations. The more you deliver on your promises, the more support you'll receive, and the easier it will be to secure ongoing investment and buy-in. Bring your experience to the forefront, work hard, support your stakeholders, and your internal reputation will naturally grow from there. And of course, support whole heartedly your own programme team, they're the real super stars of your initiative.

“

You must bring stakeholders on the journey with you. Work closely with them. Don't deliver change to them; create change with them. Remember, this is not a technology rollout, it's a change programme; a change in people, processes, and tooling.

STOTTANDMAY
CONSULTING

consulting.stottandmay.com